UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

Tiffany Roper and Heidi Emmerling, individually and on behalf of all others similarly situated *Plaintiffs*, v. Rise Interactive Media & Analytics, LLC *Defendant*.	No. 23 CV 1836 Judge Lindsay C. Jenkins

MEMORANDUM OPINION AND ORDER

Tiffany Roper and Heidi Emmerling ("Plaintiffs"), bring this putative class action against Rise Interactive Media & Analytics, LLC ("Rise" or "Defendant") based on a data breach at Rise that allegedly exposed Plaintiffs' sensitive personal information to unknown third parties. Before the Court is Defendant's motion to dismiss Plaintiffs' second amended complaint for failing to state a claim under Rule 12(b)(6). Defendant's motion is granted in part and denied in part.

I. Background

The Court recently provided a fulsome background of this case in ruling on Rise's motion to dismiss Plaintiffs' first amended complaint. [*See* Dkt. 24 at 1-4.][1] In short, Plaintiffs are the customers of Edgepark Medical Supplies, a company that sends health equipment directly to consumers. Edgepark stores its customers' personal information, such as their name, age, date of birth, home address, telephone

[1] Citations to docket filings generally refer to the electronic pagination provided by CM/ECF, which may not be consistent with page numbers in the underlying documents.

number, email address, government ID, social security number, credit card, bank account number, health insurance, medical diagnoses, and medical history. [*Id.* at 1-2.] For reasons unclear to Plaintiffs, Edgepark sent some of this information to Rise, a company that provides digital marketing services.

Rise experienced a data breach on November 14, 2022. It learned on December 2, 2022, that the accessed information may have included Edgepark's customers' information, and Rise alerted Edgepark to this fact three days later. [*Id.* at 2.] On February 10, 2023, Edgepark began alerting its customers that their "name, email address, phone number, provider information, diagnosis, expected delivery date and health insurance information", may have been compromised in the breach, but their "Social Security number, financial account information, and payment card information were **not** involved in this incident." [*Id.* at 2-3.]

Plaintiffs Roper and Emmerling are residents of South Carolina and Indiana, respectively, whose data was potentially wrongfully accessed during the breach. In either late 2022 or early 2023, Roper's insurance provider informed her someone had attempted, but failed, to use her health insurance to fill a prescription. As for Emmerling, someone attempted, but failed, to open a bank account in her name in February 2023. Both plaintiffs also allege they spent time trying to mitigate potential harm from the breach, and they experienced anxiety and concern for their loss of privacy. [*Id.* at 3.]

Plaintiffs filed their first amended complaint on June 22, 2023, claiming Rise is liable for negligence, unjust enrichment, intrusion upon seclusion, and for violating

South Carolina's Data Breach Notification Act ("SCDBNA"). [Dkt. 14.] Rise moved to dismiss, which the Court granted in part and denied in part. The Court dismissed the negligence, intrusion upon seclusion and a portion of the SCDBNA claim without prejudice; the unjust enrichment claim with prejudice; and denied the motion to dismiss a portion of Roper's SCDBNA claim. [Dkt. 24]

In response, Plaintiffs filed a second amended complaint, which alleged negligence, public disclosure of private facts, and the SCDBNA claim. [Dkt. 27.] Plaintiffs' allegations changed little, with the few new allegations focused on Rise's technological sophistication and the publicization of Plaintiffs' private information. [*See* Dkt. 28-1.] Rise has moved to dismiss all three claims on the merits.

II. Analysis

At the motion to dismiss stage, the Court takes well-pleaded factual allegations as true and draws reasonable inferences in favor of the plaintiff. *Choice v. Kohn L. Firm, S.C.*, 77 F.4th 636, 638 (7th Cir. 2023); *Reardon v. Danley*, 74 F.4th 825, 826-27 (7th Cir. 2023). "To survive a motion to dismiss under Rule 12(b)(6), plaintiff's complaint must allege facts which, when taken as true, plausibly suggest that the plaintiff has a right to relief, raising that possibility above a speculative level." *Cochran v. Ill. State Toll Highway Auth.*, 828 F.3d 597, 599 (7th Cir. 2016) (cleaned up).

A. Negligence

The sole question at issue in Plaintiffs' negligence claim is whether they have adequately pled the element of damages. The Court determines they have.

"Illinois law requires a plaintiff to plead a legally cognizable present injury or damage to sustain a negligence claim." *In re Gallagher Data Breach Litig.*, 631

F.Supp.3d 573, 587 (N.D. Ill. 2022) (internal quotations omitted). An increased risk of harm can serve as an element of damages, "but the plaintiff may not recover solely for the defendant's creation of an increased risk of harm." *Berry v. City of Chicago*, 2020 IL 124999, ¶ 38. A claim for negligence, however, "is actionable if it directly causes emotional distress." *Volling v. Antioch Rescue Squad*, 999 F. Supp. 2d 991, 999 (N.D. Ill. 2013) (citing *Corgan v. Muehling*, 574 N.E.2d 602, 608–09 (Ill. 1991) (abolishing requirement of physical manifestation of emotional distress).

In moving to dismiss Plaintiffs' negligence claim, Rise argues Plaintiffs have not suffered a present injury—Roper's fraudulent prescription was not filled, and Emmerling's fraudulent bank account was not opened. [Dkt. 28 at 8-9.] And because they have only alleged "the potential risk of future injury", their negligence claim should be dismissed. [*Id.*]; *Moyer v. Michaels Store, Inc.*, 2014 WL 3511500, at *7 (N.D. Ill. July 14, 2014) ("Illinois courts have rejected the argument that an elevated risk of identity theft constitutes actual damage for purposes of stating common law or statutory claims."); *see also Williams v. Manchester*, 888 N.E.2d 1, 13 (Ill. 2008) ("[A]s a matter of law, an increased risk of future harm is an element of damages that can be recovered for a present injury—it is not the injury itself.")

But Rise ignores Plaintiffs' allegations that they suffered anxiety and concern for loss of privacy because of the data breach.[2] [Dkt. 27 ¶¶ 63, 69.] Allegations of

[2] In fairness to Rise, Plaintiffs do not discuss this allegation either. Instead, Plaintiffs focus their response brief on the Court's prior Article III standing analysis, [Dkt. 31 at 5], which is a distinct inquiry from whether they have adequately pled a negligence claim under Illinois law. *See Leslie v. Medline Indus., Inc.*, 2021 WL 4477923 (N.D. Ill. Sept. 30, 2021) (dismissing negligence claim for lack of cognizable injury after finding plaintiff had Article

emotional harm are sufficient to state a negligence claim under Illinois law, including in the data breach context. *In re Gallagher*, 631 F.Supp.3d 573 at 587 ("There can be no dispute that Plaintiffs have alleged present injuries or damages; for instance, all allege experiencing emotional harms such as anxiety and increased concerns for the loss of privacy … [t]hese types of non-economic damages are recoverable under Illinois law"); *see also Rowe v. UniCare Life and Health Ins. Co.*, 2010 WL 86391, at *4-5 (N.D. Ill. Jan. 5, 2010). Because Plaintiffs have alleged facts, which, if proven, could satisfy the present injury requirement, Rise's motion to dismiss the negligence claim is denied.

B. Public Disclosure of Private Facts

Plaintiffs have replaced their intrusion upon seclusion claim with another privacy-based tort: public disclosure of private facts. To state this claim under Illinois law, "a plaintiff must allege that: '(1) publicity was given to the disclosure of private facts; (2) the facts were private and not public facts; and (3) the matter made public would be highly offensive to a reasonable person.'" *Anderson v. United Airlines, Inc.*, 2023 WL 5721594, at *3 (N.D. Ill. Sept. 5, 2023) (quoting *Johnson v. K Mart Corp.*, 723 N.E.2d 1192, 1197 (2000)). Public disclosure means "communicating the matter to the public at large or to so many persons that the matter must be regarded as one of general knowledge." *Doe v. Fertility Ctrs. of Ill.*, 2022 WL 972295, at *6 (N.D. Ill.

III standing). In addition, Plaintiffs' stated damages for their negligence claim do not include emotional damages, but do include damages such as "out-of-pocket expenses" for preventing identity theft and freezing credit reports that are not otherwise factually supported in the complaint. [*See* Dkt. 27 ¶¶ 108-109.] This is sloppy pleading which the Court directs Plaintiffs to correct, but it satisfies Rule 8(a)'s lenient requirements.

Mar. 31, 2022). Public disclosure can also be satisfied where there is a "disclosure to a limited number of people if those people have a special relationship with the plaintiff that makes the disclosure as devastating as disclosure to the public at large." *Id.* (quoting *Karraker v. Rent-A-Ctr., Inc.*, 411 F.3d 831, 838 (7th Cir. 2005)).

Rise concedes Plaintiffs satisfy the latter two elements but contends Plaintiff cannot satisfy the first because the data breach does not constitute a public disclosure. [Dkt. 28 at 9-10.] Plaintiffs disagree, arguing their information was disclosed to "the universe of threat actors who seek to use Plaintiffs' private facts for personal gain: namely those that would engage in identity theft", and that Plaintiffs therefore have a special relationship with these individuals. [Dkt. 31 at 6.] Rise has the better argument.

As noted in its reply, Rise did not disclose Plaintiffs' private facts to the "universe of threat actors" and Plaintiffs do not allege as much. [Dkt. 32 at 3-4.] Rather, Plaintiffs allege a nefarious third-party stole the information from Rise, and the third-party could theoretically further share their data in the future.

Courts have routinely found these allegations insufficient to qualify as a "public disclosure." *See e.g., Doe*, 2022 WL 972295, at *6 (dismissing public disclosure claim based on data breach where plaintiff alleged their information was "stolen by a third party and is now available to disclosure to others without authorization"); *White v. Citywide Title Corp.*, 2018 WL 5013571, at *3 (N.D. Ill. Oct. 16, 2018) (dismissing plaintiff's public disclosure claim after holding defendant did not give publicity to plaintiff's information through data breach); *In re Barnes & Noble Pin Pad Litig.*,

2016 WL 5720370, at *7 (N.D. Ill. Oct. 3, 2016) (same), *vac'd on other grounds*, 887 F.3d 826, (7th Cir. 2018); *Maglio v. Advocate Health & Hosps. Corp.*, 2015 IL App (2d) 140782, ¶ 31 (same); *Dolmage v. Combined Ins. Co. of Am.*, 2015 WL 292947, at *10 (N.D. Ill. Jan. 21, 2015) (when plaintiff's "information was stolen from a third-party vendor", dismissal is proper for a public disclosure claim because defendant "did not communicate the information to the public at large.").

Plaintiffs criticize this caselaw arguing these courts did not meaningfully analyze the "special relationship" theory of public disclosure Plaintiffs allege here. [Dkt. 31 at 6-7.] But Plaintiffs have not alleged how their relationship with the hacker(s)—whose identity is unknown—is different than the plaintiffs in *Doe*, or the other data breach cases cited by the Court. Plaintiffs' relationship is not made "special" by the mere fact that the bad actors have Plaintiffs' information and can attempt to use it or sell it to others in the future. *Doe*, 2022 WL 972295, at *6. Nor is Plaintiffs' claim saved by citing to *Flores*, a case that did not involve a claim for public disclosure of private facts. *See Flores*, 2023 IL App (1st) 230140, at ¶¶ 49-53.[3] Because Plaintiffs have not alleged facts which would permit the inference Rise made a public disclosure of Plaintiffs' private information, the claim is dismissed.

C. South Carolina's Data Breach Notification Act

Finally, Rise has moved to dismiss Roper's SCDBNA claim, which Roper clarified is only a subsection "B" claim. [Dkt. 27 at 24.] This subsection requires those "conducting business in this State and maintaining … personal identifying

[3] *Flores* involved a claim for intrusion upon seclusion, the invasion of privacy tort Plaintiffs initially attempted to plead.

information that the person does not own" to "notify the owner or licensee of the information of a breach of the security of the data immediately following discovery, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person." S.C. Code § 39-1-90(B). The Court previously held this claim could proceed because Rise did not "immediately" inform either Edgepark (72 hours) or Roper (over two months). [Dkt. 24 at 20.]

Defendant raises two arguments for why the SCDBNA claim should be dismissed: Rise does not conduct business in South Carolina, and it immediately notified Edgepark of the data breach. [Dkt. 28 at 10-12.] The Court disagrees.

Rise argues it does not conduct business in South Carolina because it is incorporated in Delaware, has its principal place of business in Illinois, and is not licensed to do business in South Carolina.[4] [Dkt. 28 at 10-11.] The Court cannot conclude these factors establish Rise does not "conduct business" in South Carolina, and Rise has pointed to no authority to support its argument.

Nor does it follow logically that Rise's failure to register as a business in South Carolina means it does not conduct business in South Carolina. Rise could serve clients located in South Carolina, for example. At minimum, it cannot be disputed Rise collects the personal identifying information of South Carolinians, presumably to help its clients market to them. [*See* Dkt. 27 at 4-5.] This may very well satisfy the

[4] Rise included a link to the South Carolina Secretary of State's business records search, which the Court can take judicial notice of as a public record without converting this into a motion for summary judgment. *Ronald D. Fosnight & Paraklese Techs., LLC v. Jones*, 41 F.4th 916, 922 (7th Cir. 2022).

"conducting business" requirement of SCDBNA, which was presumably enacted to protect South Carolinians in the event of a data breach.

Rise's second argument that it immediately informed Edgepark of the data breach is equally unavailing in this motion as it was in the last. Rise learned of the data breach on a Friday, December 2, 2022. Rise informed Edgepark of the breach the next business day, Monday, December 5, 2022. [Dkt. 28 at 12.] The statute requires the target of a data breach to notify the owner or licensee "immediately following discovery." Waiting three days—when the bad actors could very well be misusing the stolen information of ignorant consumers—does not constitute immediacy as a matter of law. Roper's SCDBNA claim may proceed.

III. Conclusion

For the foregoing reasons, Rise's motion to dismiss Plaintiffs' negligence claim, and Roper's SCDBNA claim is denied. Rise's motion to dismiss Plaintiffs' public disclosure of private facts claim is granted. And because Plaintiffs cannot allege the data breach incident constitutes a "public disclosure", the dismissal is with prejudice.

Notwithstanding the denial of Rise's motion with respect to the negligence claim, within 14 days of this Order, Plaintiffs are directed to file a third amended complaint (with a redline as stated in the Court's standing order) that clarifies their damages allegations with respect to the negligence claim; the Court will set a date for Defendant's to answer.

Enter: 23 CV 1836
Date: April 10, 2024

Lindsay C. Jenkins
United States District Judge